AMENDMENTS TO THE SPECIFICATION:

Please replace the paragraph on page 5, lines 4-5, with the following amended paragraph.

FIGS. ~~2-5~~ 2-6 are flow-chart representations of some steps performed in one implementation of one embodiment of the present invention.

Please replace the paragraph beginning on page 14, line 17, and ending on page 15, line 2, with the following amended paragraph.

The central sign-on server 32 then creates a digital signature on all information to be communicated by the central sign-on server 32 (step 306). In the preferred implementation, the central sign-on server 32 uses its private key to create the digital signature. The central sign-on server 32 then redirects the client browser 42 back to the web server 20 (step 308). The redirect includes parameters in the query string, including the log-in identification on the web server 20 associated with the client browser 42, the challenge, and the digital signature of the central sign-on server 32 on all of this information (step 308). The client browser 42 responds to the redirect by sending the request to the web ~~browser~~ server 20.

Please replace the paragraph on page 15, lines 3-10, with the following amended paragraph.

The web ~~browser~~ server 20 verifies the digital signature of the central sign-on server 32 (step 310). The web ~~browser~~ server 20 receiving the information forwarded by the central sign-on server 32 indicating that a current session is noted for that client browser 42 on a different federation server, creates a local session on the web server 20 for the client browser 42 (step 312). Having verified the central sign-on server's signature, the web server 20 is assured that a current session is in place for that client browser 42 on one of the federation servers. The web server 20 may thus initiate a local session for the client browser 42 without the need for the client browser 42 to provide authentication.

Please replace the paragraph beginning on page 16, line 21, and ending on page 17, line 7, with the following amended paragraph.

Additionally, the web server 20 occasionally runs a session freshening task for all active sessions (step 512). All sessions, including but not limited to newly created

sessions under the initial log-on steps 300, or the transparent session establishment steps 400, are subject to the session freshening task of step 512 of FIG. 5~~(step 510)~~. Each server in the federation runs such a freshening task in the background. In a preferred implementation this session freshening task looks through a list of sessions contained on the web server 20 for any sessions that are due to expire on the central sign-on server 32 before the next time the session freshening task runs. For each such session, if the delta between the current time and the last accessed time is less than the recorded session expiration duration, then the session is considered current and is assembled into a list of sessions that need to be freshened on the central sign-on server (see step 508, 512).

Please replace the paragraph beginning on page 17, line 23, and ending on page 19, line 8, with the following amended paragraph.

FIG. 6 is a flow-chart representation of selected basic generic steps for explicit session termination 600 of one implementation of the present invention. The steps 600 generally describe the way in which the present invention ensures that a client who logs out or terminates the session on one server in the federation, has sessions terminated on all of the servers in the federation. The client browser 42 terminates the session with the web server 20 or logs out of the web server 20 (step 602). The web server 20 looks up the challenge associated with that session from a record located on the web server 20, and terminates the local session on the web server 20 (step 604). The web server 20 sends a message to the central sign-on server 32 for each federation to which the web server 20 belongs (step 606). In the preferred implementation, the message is an encrypted HTTP message containing at least the challenge generated by the web server at the creation of the session for that client browser 42, the web browser's server identification, a parameter indicating that the session on the web ~~browser~~ server 20 has been explicitly terminated, and the digital signature of the web server 20 on all of this information (step 606). The central sign-on server 32 verifies the digital signature of the web server 20 (step 608). The central sign-on server 32 preferably uses the challenge sent by the web ~~browser~~ server 20 in step 606 to look up on the central sign-on server 32 the record of any current sessions associated with the client browser 42 (step 610). For each federation server with a current session for the client browser 42, the central sign-on server 32 removes the record on the central sign-on server 32 for that session (step 612). The central sign-on server 32 then sends a message to each federation

server for which the client browser 42 had a local session (step 614). In one implementation, the message to each federation server is an HTTP message including the challenge generated by the federation server in the creation of the local session on that federation server, a parameter indicating that the session has been explicitly terminated, and the central sign-on server's private digital signature on all of this information. Each federation server receiving a message from the central sign-on server 32 verifies the digital signature of the central sign-on server 32 (step 616). After verifying the digital signature of the central sign-on server 32, each federation server receiving a message terminates the local session on the federation server associated with the challenge (step 618). In this fashion, the client/user is insured that his sessions have been terminated at each federation server that he may have visited for each federation, and that any confidential or sensitive information can not be accessed by accident due to a connection or session left open under that client's username.